Available online at www.sciencedirect.com

ScienceDirect

Procedia Engineering 140 (2016) 8 – 11

Procedia Engineering

www.elsevier.com/locate/procedia

MRS Singapore – ICMAT Symposia Proceedings

8th International Conference on Materials for Advanced Technologies

All-Optical Parallel Encryption of QPSK Signals Based on Non-Degenerate Four Wave Mixing in HNLF for Physical Layer Security of Optical Network

Min Zhang* , Yue Cui*, Yueying Zhan, Danshi Wang,Xue Chen

State Key Lab. of Information Photon. and Opt. Commun., Beijing Univ. of Posts & Telecom., Beijing 100876, China

Abstract

A scheme for all-optical encryption/decryption of QPSK signals based on ND-FWM in HNLF is proposed. Theoretical analyses and simulations are conducted. The results are useful for designing optical encryption/decryption for complex modulated signals.

Selection and/or peer-review under responsibility of the scientific committee of Symposium 2015 ICMAT

Keywords: Fiber optics communications; All-optical networks; Nonlinear optical signal processing.

1. Introduction

With respect to the physical layer of optical networks, encryption/decryption based on optical signal processing is promising because it supports direct and ultrafast physical-layer cryptography. Several approaches have been proposed to enhance the security of the optical network in optical domain[1-3], most of which are based on XOR or other logic gates, it resulted in a not very high degree of confidentiality.

In this paper, we propose a scheme for all-optical parallel encryption of QPSK signals based on non-degenerate four-wave mixing (ND-FWM) in Highly Non-linear Fiber (HNLF) for optical network security. Theoretical analysis and simulations are conducted to verify the proposal. The encryption is realized by employing-ND-FWM among three QPSK signals in HNLF. The parallel three signals can be encrypted in phase flexibly. Each of the three signals can be regarded as the pre-encryption signal and the other two signals are used as the keys during data transmission. The scheme inherently provides a more confidential and flexible encryption solutions in all-optical network.

Selection and/or peer-review under responsibility of the scientific committee of Symposium 2015 ICMAT
doi:10.1016/j.proeng.2015.09.236

2. Operation principle

To encrypt the parallel QPSK signals, we apply the ND-FWM in HNLF because FWM is a phase and intensity preserving process and thus suitable for multiple all-optical format conversions. Besides, ND-FWM in HNLF ND -FWM has the characteristics of low latency and high speed. In fact, both D-FWM and ND-FWM may occur in HNLF, resulting in several new components, as schematically illustrated in Fig. 1[4].

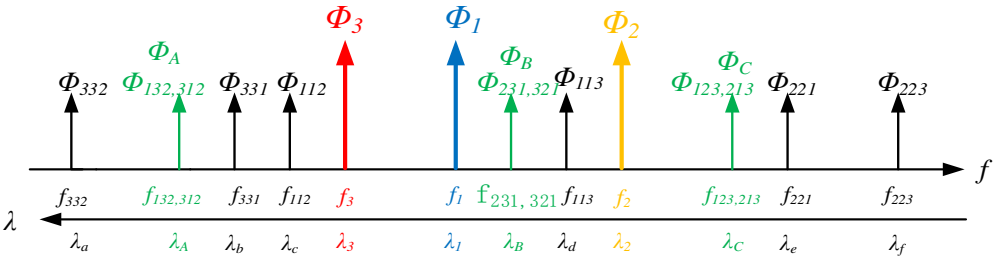

Fig. 1. Schematic illustration of the FWM transfer process in HNLF.

The three input QPSK signals are at wavelengths λ_1, λ_2 and λ_3 respectively. Each of the generated idlers possesses a frequency of $f_{lmn}=f_l+f_m-f_n$ and a phase of $\Phi_{lmn}=\Phi_l+\Phi_m-\Phi_n$, where l,m and n are unequal to each other and belong to {1,2,3} [4].The generated ND-FWM components with wavelengths of λ_A, λ_B and λ_C, , and phases of Φ_A,Φ_B andΦ_C are chosen as the encrypted signals. For example, if we assume QPSK1@λ_1 as the pre-encryption signal, QPSK2@λ_2 and QPSK3@λ_3 become the dual-key signals. Therefore, the generated idler which is at the wavelength of λ_C is identified as the encrypted signal, with a frequency of $f_{123,\,213}=f_1+f_2-f_3$ and a phase of $\Phi_C=\Phi_{123,213}=\Phi_1+\Phi_2-\Phi_3$. During the encryption process, the change of constellation of QPSK1 is shown in Fig. 2.

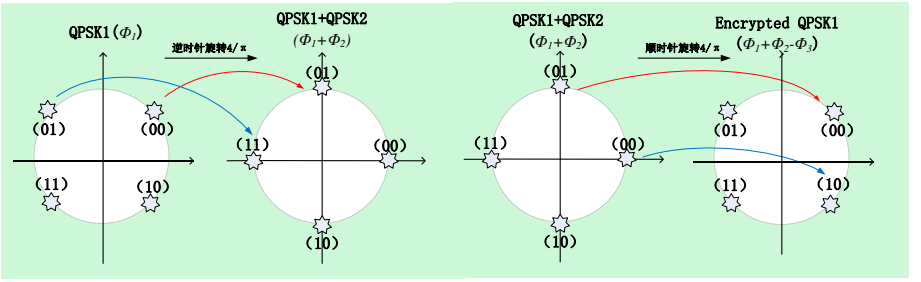

Fig. 2. The change of constellation of QPSK1

The true table for encrypted QPSK1 is calculated in Table.1. Based on this relationship, the logic expressions for the encryption process are given as Equations (1)~(4).At the same time, other two QPSK signals are also encrypted in HNLF1, which QPSK1@λ1 is acted as key signal. In decryption process, a second ND-FWM in HNLF2 is used among the generated idlers, namely the encrypted signal, and two keys which are QPSK2 and QPSK3 in this case. Through the encryption process, we can obtain the decrypted signal with the phase of Φ1=ΦC+Φ3-Φ2=Φ1+Φ2-Φ3+Φ3-Φ2=Φ1 and the wavelength of λ1， namely QPSK1signal. Therefore, encryption and decryption process all are completed.

Table.1.True table for the encrypted QPSK1 signal

QPSK4 b4[c41, c42, (Φ1+Φ2)]		*QPSK2 b2 [c21, c22, (Φ2)]*			
		00(π/4)	01(3π/4)	11(5π/4)	10(7π/4)
QPSK1 b1 [c11, c12, (Φ1)]	00(π/4)	01(π/2)	11(π)	10(3π/2)	00(2π)
	01(3π/4)	11(π)	10(3π/2)	00(2π)	01(π/2)
	11(5π/4)	10(3π/2)	00(2π)	01(π/2)	11(π)
	10(7π/4)	00(2π)	01(π/2)	11(π)	10(3π/2)

Encrypted Signal b5[c51, c52, (Φ1+Φ2-Φ3)]		*QPSK4 b4 [c41, c42, (Φ1+Φ2)]*			
		00(2π)	01(π/2)	11(π)	10(3π/2)
QPSK3 b3[c31,c32, (Φ3)]	00(π/4)	10(7π/4)	00(π/4)	01(3π/4)	11(5π/4)
	01(3π/4)	11(5π/4)	10(7π/4)	00(π/4)	01(3π/4)
	11(5π/4)	01(3π/4)	11(5π/4)	10(7π/4)	00(π/4)
	10(7π/4)	00(π/4)	01(3π/4)	11(5π/4)	10(7π/4)

$$c_{41}=\bar{c}_{21}(\bar{c}_{12}\bar{c}_{22}+\bar{c}_{11}c_{22})+c_{21}(\bar{c}_{12}c_{22}+\bar{c}_{11}\bar{c}_{22}) \quad (1)$$

$$c_{42}=\bar{c}_{21}(\bar{c}_{11}\bar{c}_{22}+\bar{c}_{12}c_{22})+c_{21}(\bar{c}_{11}c_{22}+\bar{c}_{12}\bar{c}_{22}) \quad (2)$$

$$c_{51}=\bar{c}_{41}(\bar{c}_{31}\bar{c}_{42}+\bar{c}_{32}c_{42})+c_{41}(\bar{c}_{31}c_{42}+\bar{c}_{32}\bar{c}_{42}) \quad (3)$$

$$c_{52}=\bar{c}_{41}(\bar{c}_{32}\bar{c}_{42}+\bar{c}_{31}c_{42})+c_{41}(\bar{c}_{32}c_{42}+\bar{c}_{31}\bar{c}_{42}) \quad (4)$$

3. Simulations and results

The simulation platform used in this study is VPI Transmission Maker TM8.6 Optical Systems. Figure 3 shows the system setup of the optical encryption and decryption in the simulations.

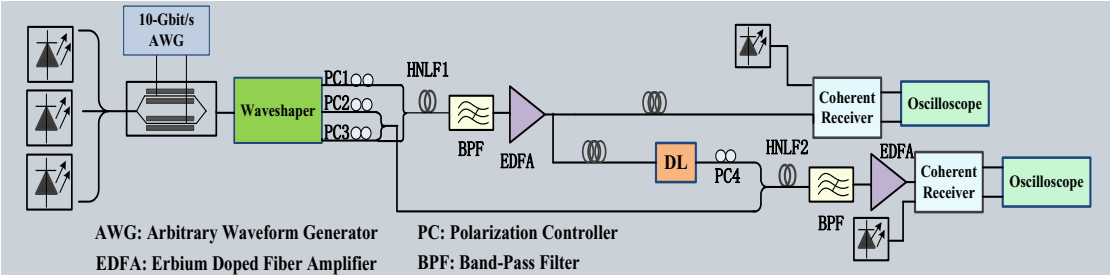

Fig. 3. Simulation setup for optical parallel QPSK encryption/decryption

The optical parallel QPSK signals (i.e. b1, b2 and b3) are generated by modulating a continuous wave (CW) at 1553.59 nm, 1554.01 nm and 1552.99 nm in a dual-parallel lithium neonate (LiNbO3) modulator with two 10-Gbps de-correlated and non-return-to-zero (NRZ) pseudo-random binary sequences (PRBSs) with a length of 231-1. b1, b2 and b3 are amplified and then de-multiplexed by a dual-output optical Gaussian filter (Finisar Waveshaper 4000s). b2and b3 are split into two portions. One portion is mixed with b1 and injected into HNLF1 after passing the polarization controller. The encryption signal is obtained from the first ND-FWM in HNLF1, and therefore, b1 is encrypted as b5. After the amplifier and band-pass filter, b2, b3 and b5 are transmitted through different fiber links and adjusted in phase before entering HNLF2, where the second ND-FWM occurs and b5 are decrypted and observed through an oscilloscope. The HNLF used in this scheme has a length of 1 km, a nonlinear coefficient of 10 W-1/km, an attenuation coefficient of 0.2dB/km, and a dispersion slope of 0.03 ps/nm2/km.

The simulated spectra of the outputs of HNLF1 and HNLF2 are shown in Fig. 4, in which encrypted signal b5 is shifted to a new generated frequency; the decrypted signal, after amplification, matches the original input signal b1 to a large degree. The BER is plotted as a function of the optical signal-to-noise ratio (OSNR) in Fig. 5. The results indicate that, to achieve a BER lower than 10-3, the OSNR of encrypted signal should be larger than 14 dB, and the OSNR of the decrypted signal should be larger than 18.5 dB.

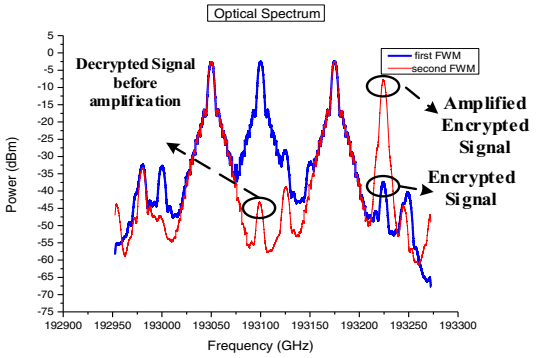

Fig. 4. Spectra of the outputs of HNLF, with blue curves for HNLF1 and red curves for HNLF2.

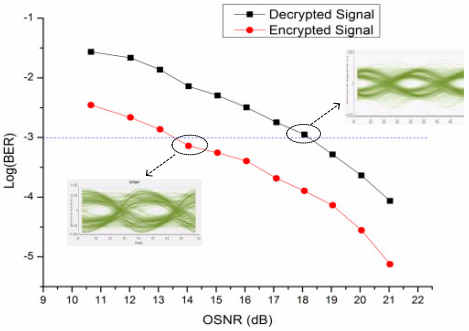

Fig. 5. BER with respect to the OSNR of the encrypted and the decrypted QPSK signals.

The constellations of b1, encrypted signal, and the decrypted signal are shown in Fig. 5. Both the evolutions of the spectra in Fig.4 and the constellations in Fig. 6 indicate that the proposed scheme for optical encryption/decryption of QPSK signal works.

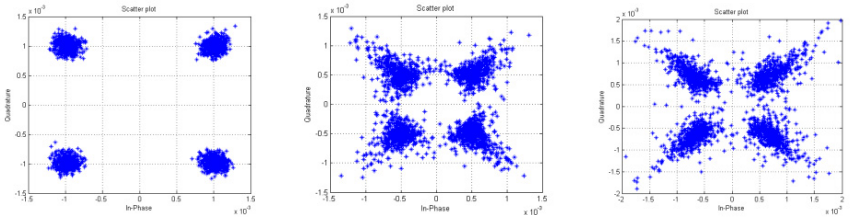

Fig. 6 Constellations of the original, encrypted, and decrypted QPSK signals: (a) constellation of the original signal; (b) constellation of the encrypted signal; and (c) constellation of the decrypted signal..

4. Conclusion

We have proposed a scheme for all- optical encryption/decryption of parallel QPSK signals based on ND-FWM in HNLF. Simulation results show that the scheme can offers a compact and ultra-fast approach to the confidential transmission of parallel QPSK signals in optical networks.

Acknowledgements

This study is supported by NSFC Project No.61372119, 863 Program No.2012AA011302, Doctoral Scientific Fund Project of the Ministry of Education of China N0.20120005110010, and BUPT Excellent Ph.D. Students Foundation.

References

[1] B. Wu, A. Agrawal, I. Glesk, E. Narimanov, S. Etemad, and P. Prucnal, “Steganographic fiber-optic transmission using coherent spectral phase-encoded optical CDMA,” Conference on Lasers and Electro-Optics, CFF5, May 2008.
[2] J. M. Castro, I. B. Djordjevic, and D. F. Geraghty,“Novel super structured Bragg gratings for optical encryption,” IEEE J. Lightw. Technol vol. 24, iss. 4, pp. 1875 – 1885, April 2006.
[3] M. P. Fok, K. Kravtsov, Y. Deng, Z. Wang, T. Wang, and P. R. Prucnal, “Securing data networks using optical signal processing,” International Conference on Photonics in Switching, invited S-03-5, Sapporo, Japan, August 2008.
[4] B. Wu, S. Fu, J. Wu, P. Shum, N.Q. Ngo, K. Xu, X. Hong, J. Lin, “40 Gb/s Multifunction Optical Format Conversion Module With Wavelength Multicast Capability Using Nondegenerate Four-Wave Mixing in a Semiconductor Optical Amplifier,” Journal of Lightwave Technology, p. 4446-4454, October 2009.